UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/037,267	01/02/2002	Tom Howard	10011529-1	6181

7590 05/08/2008

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER
BROWN, CHRISTOPHER J

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
05/08/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte TOM HOWARD and TIM GOLDSTEIN

Appeal 2007-3624
Application 10/037,267
Technology Center 2100

Decided: May 8, 2008

Before LANCE LEONARD BARRY, HOWARD B. BLANKENSHIP, and THU ANN DANG, *Administrative Patent Judges*.

BARRY, *Administrative Patent Judge*.

DECISION ON APPEAL

I. STATEMENT OF THE CASE

A Patent Examiner rejected claims 1-7, 9, and 11-19. The Appellants appeal therefrom under 35 U.S.C. § 134(a). We have jurisdiction under 35 U.S.C. § 6(b).

A. INVENTION

1The invention at issue on appeal prevents unauthorized use of a wireless device. (Spec. 1.) When a cellular telephone is stolen, its owner may notify his cellular provider. The cellular provider will update its records to indicate that the telephone is invalid. Anyone who attempts to use the telephone thereafter will be denied access to any cellular network. (*Id.* 2.)

This approach is problematic for other wireless devices. Many commercially-available wireless devices, e.g., personal data assistants (PDAs), perform a variety of functions. If the security protocols of traditional cellular telephones were applied to wireless PDAs, a thief who has stolen a wireless PDA could not use the PDA for wireless communication but could use it to execute other software applications. (*Id.*)

In contrast, the Appellant's wireless device features a processor for executing at least one user application and a wireless communication subsystem for transmitting and receiving data. When the device receives a message indicating it is not in possession of a rightful user, a security protocol process prevents execution of the user application. (*Id.* 3.)

B. Illustrative Claim

Claim 1, which further illustrates the invention, follows.

1. A processor-based device that prevents unauthorized use, comprising:

a processor for executing software instructions;

software instructions defining at least one user application;

a wireless communication subsystem that is operable to transmit and receive data utilizing a wireless protocol;

software instructions defining a security protocol process that is operable to prevent execution of said software instructions defining said at least one user application by said processor when a message is received via said wireless communication subsystem, wherein said message indicates that said processor-based device is not in possession of a rightful user; and

a basic input/output system (BIOS) that is operable to boot said processor-based device and is further operable to verify integrity of said security protocol process before completing boot operations.

C. Rejection

Claims 1-7, 9, and 11-19 stand rejected under 35 U.S.C. § 103(a) as obvious over U.S. Patent No. 5,987,609 ("Hasebe"); U.S. Application Pub. No. 2002/0004905 ("Davis"); and U.S. Patent Application Pub. No. 2001/0045884 ("Barrus").

II. CLAIMS 1-7

"Rather than reiterate the positions of the parties *in toto*, we focus on an issue therebetween." *Ex parte Kuruoglu*, No. 2007-0666, 2007 WL 2745820, at *2 (BPAI 2007). Admitting that "Hasebe . . . fails to teach checking the integrity of the system prior to booting for identification of a tampered system" (Ans. 3), the Examiner makes the following finding.

> [W]hen the security protocol of Hasebe is included within the BIOS level implementation of the Davis system a BIOS (Davis Fig 5) as indicated within claim 1 wherein the BIOS is operable to boot the device, verify the integrity (Davis paragraph 23) of said security protocol process before completing boot operations is provided.

(*Id.* 7) The Appellants argue, "Davis does not teach or suggest a BIOS that is operable to verify integrity of a security protocol." (App. Br. 6.) Therefore, the issue is whether the Appellants have shown error in the Examiner's finding that teachings from Hasebe and Davis would have suggested BIOS verifying the integrity of a security process, which prevents execution of a user application responsive to receipt of a message via a wireless communication subsystem.

"Both anticipation under § 102 and obviousness under § 103 are two-step inquiries. The first step in both analyses is a proper construction of the claims . . . . The second step in the analyses requires a comparison of the

properly construed claim to the prior art." *Medichem, S.A. v. Rolabo, S.L.*, 353 F.3d 928, 933 (Fed.Cir. 2003) (internal citations omitted).

A. Claim Construction

"The Patent and Trademark Office (PTO) must consider all claim limitations when determining patentability of an invention over the prior art." *In re Lowry*, 32 F.3d 1579, 1582 (Fed. Cir. 1994) (citing *In re Gulack*, 703 F.2d 1381, 1385 (Fed. Cir. 1983)).

1 Here, claim 1 recites in pertinent part the following limitations:

> software instructions defining a security protocol process that is operable to prevent execution of said software instructions defining said at least one user application by said processor when a message is received via said wireless communication subsystem, wherein said message indicates that said processor-based device is not in possession of a rightful user; and
>
> a basic input/output system (BIOS) that is operable to boot said processor-based device and is further operable to verify integrity of said security protocol process before completing boot operations.

Considering all the limitations, the independent claim requires BIOS verifying the integrity of a security process, which prevents execution of a user application responsive to receipt of a message via a wireless communication subsystem.

B1. OBVIOUSNESS ANALYSIS

In rejecting claims under 35 U.S.C. § 103, the examiner bears the initial burden of presenting a *prima facie* case of obviousness." *In re Rijckaert*, 9 F.3d 1531, 1532 (Fed. Cir. 1993) (citing *In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992)). "'A *prima facie* case of obviousness is established when the teachings from the prior art itself would appear to have suggested the claimed subject matter to a person of ordinary skill in the art.'" *In re Bell*, 991 F.2d 781, 783 (Fed. Cir. 1993) (quoting *In re Rinehart*, 531 F.2d 1048, 1051 (CCPA 1976)).

Here, the paragraph of Davis cited by the Examiner explains that a "[s]torage device 170_1 contains actual Basic Input/Output System (BIOS) code 180 for execution by processing unit 110 . . . ." (¶ 0023) The paragraph does not teach, however, that the BIOS code "verif[ies] the integrity" (Ans. 7) of any security process. To the contrary, we agree with the Appellants that "Davis teaches a system that authenticates BIOS code, rather than a BIOS that verifies integrity of a security protocol." (App. Br. 6.) Specifically, the reference teaches that its "second IC [i.e., integrated circuit] device includes logic circuitry to execute a software code to authenticate the BIOS code before permitting execution of the BIOS code by the host processor." (Abs. ll. 14-17.)

Because the Examiner admits that Hasebe fails to check the integrity of its system before booting (Ans. 2), and Davis uses a security process to

verify the integrity of BIOS, rather than using the BIOS to verify integrity of a security process, we are unpersuaded that the combined teachings of the references would have suggested BIOS verifying the integrity of a security process, which prevents execution of a user application responsive to receipt of a message via a wireless communication subsystem. The Examiner does not allege, let alone show, that the addition of Barrus cures the aforementioned deficiency of Hasebe and Davis.

The Appellants have shown error in the Examiner's finding that teachings from Hasebe and Davis would have suggested BIOS verifying the integrity of a security process, which prevents execution of a user application responsive to receipt of a message via a wireless communication subsystem. Therefore, we reverse the rejection of claim 1 and of claims 2-7, which depend therefrom.

III. CLAIMS 16-19

The Examiner makes the following finding.

> As disclosed the system teaches that the BIOS must be loaded prior to operation (Davis paragraph 10). A BIOS in the context of this rejection is considered to be a basic operating system. The security program is operative to run once the system has been authenticated as described by Davis, thus being implemented in the BIOS to prevent unauthorized use (Hasebe Col 2 lines 26-36 Fig 10).

(Ans. 8.) The Appellants argue that "as noted above, Davis teaches that a cryptographic device authenticates the BIOS and does not teach or suggest a security process implemented in or by the BIOS." (Reply Br. 9.) Therefore, the issue is whether the Appellants have shown error in the Examiner's finding that teachings from Hasebe and Davis would have suggested implementing in an operating system a security process that prevents execution of a user application responsive to receipt of a message via a wireless communication subsystem.

A. Claim Construction

1 Claim 16 recites in pertinent part the following limitations:

> means for preventing execution of said software instructions defining said at least one user application by said means for processing when a message is received via said means for transmitting and receiving, wherein said message indicates that said system is not in possession of a rightful user, wherein said means for preventing execution is implemented by an operating system of said system.

In other words, the independent claim requires implementing in an operating system a security process that prevents execution of a user application responsive to receipt of a message.

B1. Obviousness Analysis

Here, the paragraph of Davis cited by the Examiner explains that its "cryptographic device authenticates software code, loaded into the cryptographic device during a boot procedure, before permitting the host processor to execute the software code." (¶ 0010.) The "software code" is the BIOS code discussed regarding claims 1-7 *supra*.

The reference further explains that its "second IC device 520 includes internal memory 525 . . . ." (¶ 0029.) For its part, the "[i]nternal memory 525 contains firmware 526 which is a small computer [security] program executed by first IC device 500 for initialization and authentication purposes in order to ensure that the firmware [i.e., the BIOS code] in storage element [170_1] . . . has not been tampered with or corrupted." (¶ 0030) Because Davis stores the BIOS code in its storage device while storing the security program in its second IC device, we are unpersuaded that the reference teaches implementing a security process in an operating system.

For its part, the paragraph of Hasebe cited by the Examiner mentions "a security process corresponding to the security level stored by the security level storing means." (Col. 2, ll. 35-36.) By relying on Davis' BIOS as an operating system, however, the Examiner implicitly concedes that Hasebe does not implement its security process in an operating system.

The Examiner does not allege, let alone show, that the addition of Barrus cures the aforementioned deficiency of Hasebe and Davis. The Appellants have shown error in the Examiner's finding that teachings from Hasebe and Davis would have suggested implementing in an operating system a security process that prevents execution of a user application responsive to receipt of a message. Therefore, we reverse the rejection of claim 16 and of claims 17-19, which depend therefrom.

IV. CLAIMS 9, 11, 12, 14, AND 15

> 1When multiple claims subject to the same ground of rejection are argued as a group by appellant, the Board may select a single claim from the group of claims that are argued together to decide the appeal with respect to the group of claims as to the ground of rejection on the basis of the selected claim alone. Notwithstanding any other provision of this paragraph, the failure of appellant to separately argue claims which appellant has grouped together shall constitute a waiver of any argument that the Board must consider the patentability of any grouped claim separately.
>
> 37 C.F.R. § 41.37(c)(1)(vii) (2005).

Here, the Appellants argue claims 9, 11, 12, 14, and 15, which are subject to the same ground of rejection, as a group. (App. Br. 9-10). We select claim 9 as the sole claim on which to decide the appeal of the group.

The Examiner makes the following findings.

> [H]asebe teaches the use of RAM, in combination with the systems of Davis (Davis paragraph 30, Fig 5) and Barrus (Barrus paragraph 16) this system uses Flash memory, as the system of Barrus utilizes flash for all program functions. Additionally, as taught by the combination the BIOS (Davis paragraph 23, 30) is contained within ROM, similar to that of the security protocol of Hasebe (Fig 3) and settings, which are contained in RAM, wherein from the teachings of the combination these stores are combined as the same. The system of Hasebe teaches storing settings of the security program in RAM, however, RAM is volatile memory and does not retain information with a loss of power, therefore, the combination teaches storing such features in non-volatile memory (Davis paragraph 30, Barrus paragraph 16).

(Ans. 7-8.) He further finds that "it can be seen from Hasebe Fig 3 part 23 that incoming messages are stored (Col 4 lines 53-65, Col 5 line 65 - Col 6 line 3), and by the teachings of the rejection are stored in non-volatile memory." (*Id.* 9.) The "Appellant acknowledges the Examiner's arguments on pages 7 and 9 of the Answer, but notes that even if the allegations about the teaching of Barrus is true, arguendo, there is still a lack of motivation provided thus far for combining Barrus with the other references." (Reply Br. 8.) Therefore, the issue is whether the Appellants have shown error in the Examiner's rejection of claim 9.

"Silence implies assent." *Harper & Row Publishers, Inc. v. Nation Enters.,* 471 U.S. 539, 572 (1985)). Here, the Appellants do not contest the

Examiner's findings about what Hasebe, Davis, and Barrus teach. Their silence implies their assent to these findings.

Furthermore, 1"it is inappropriate for appellants to discuss in their reply brief matters not raised in . . . the principal brief[ ]. Reply briefs are to be used to reply to matter[s] raised in the brief of the appellee." *Kaufman Company, Inc. v. Lantech, Inc.*, 807 F.2d 970, 973 n. (Fed. Cir. 1986). "Considering an argument advanced for the first time in a reply brief . . . is not only unfair to an appellee . . . but also entails the risk of an improvident or ill-advised opinion on the legal issues tendered." *McBride v. Merrell Dow and Pharms., Inc.*, 800 F.2d 1208, 1211 (D.C. Cir. 1986) (internal citations omitted).

> There are cogent reasons for not permitting an appellant to raise issues or arguments in a reply brief. Among them are the unfairness to the appellee who does not have an opportunity to respond and the added burden on the court that a contrary practice would entail. As the Tenth Circuit put it, permitting an appellant to raise new arguments in a reply brief "would be unfair to the court itself, which without the benefit of a response from appellee to an appellant's late-blooming argument, would run the risk 'of an improvident or ill-advised opinion, given [the court's] dependence . . . on the adversarial process for sharpening the issues for decision.'" *Headrick* [*v. Rockwell Int'l Corp.*], 24 F.3d [1272,] 1278 [(10th Cir. 1994)], (quoting *Herbert v. Nat'l Academy of Sciences*, 974 F.2d 192, 196 (D.C. Cir. 1992).

Carbino v. West, 168 F.3d 32, 34-35 (Fed. Cir. 1999)

Here, the Appellants' Reply Brief presents new arguments regarding "a lack of motivation . . . for combining Barrus with the other references." (Reply Br. 8.) Because the reason given on page 4 of the Examiner's Answer why "[i]t would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the system of Barrus et al with that of the Hasebe/Davis combination" is verbatim to that on page 3 of the Final Rejection, we find nothing in the Answer that would have prompted the arguments.

The arguments concerning motivation could have been made in the Appellants' Appeal Brief. The term "reply brief" is exactly that, a brief in reply to new rejections or new arguments set forth in an examiner's answer. The Appellants may not present their arguments in a piecemeal fashion, holding back arguments until a patent examiner answers their original brief. Of course, the Appellants may present new arguments directly to the Examiner for consideration as part of a continuing application.

The Appellants have shown no error in the Examiner's rejection of claim 9. Therefore, we affirm the rejection of claim 9 and of claims 11, 12, 14, and 15, which fall therewith.

V. CLAIM 13

The Examiner makes the following findings.

> Hasebe discloses an owner indication option that when the device is not in possession of the rightful owner the system displays the owners name and address (Hasebe Fig 6, 12, Col 6 lines 44-46, 49-51, Col 10 lines 20-22), a message that indicates the current user is not the rightful user is thus indicated by displaying the rightful owner's information.

(Ans. 8.) The Appellants argue, "Indicating an owner name and telephone number indicates just that — an owner name and telephone number. It is not enough, without more, to teach or suggest presenting 'information indicating that said rightful user is not in possession.'" (Reply Br. 8.) Therefore, the issue is whether the Appellants have shown error in the Examiner's finding that Hasebe displays a message on a display of a processor-based device.

A. Claim Construction

"An intended use or purpose usually will not limit the scope of the claim because such statements usually do no more than define a context in which the invention operates." *Boehringer Ingelheim Vetmedica, Inc. v. Schering-Plough Corp.*, 320 F.3d 1339, 1345, 65 USPQ2d 1961, 1965 (Fed.Cir. 2003). Although "[s]uch statements often . . . appear in the claim's preamble," *In re Stencel*, 828 F.2d 751, 754, 4 USPQ2d 1071, 1073

(Fed.Cir. 1987), a statement of intended use or purpose can appear elsewhere in a claim. *Id.*

Here, claim 13 recites in pertinent part the following limitations: "displaying a message on a display of said processor-based device to indicate that said processor-based device is not in possession of said rightful user." Because the prepositional phrase "to indicate that said processor-based device is not in possession of said rightful user" merely states an intended use or purpose for the message, the phrase is not entitled to patentable weight. Giving the claim its broadest, reasonable construction, therefore, the limitations require displaying a message on a display of a processor-based device.

B1. Obviousness Analysis

The question of obviousness is "based on underlying factual determinations including . . . what th[e] prior art teaches explicitly and inherently . . . ." *In re Zurko*, 258 F.3d 1379, 1383-84 (Fed. Cir. 2001) (citing *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966); *In re Dembiczak*, 175 F.3d 994, 998 (Fed. Cir. 1999); *In re Napier*, 55 F.3d 610, 613 (Fed. Cir. 1995)).

Here, the Appellants admit that Hasebe "that the owner indication feature displays the identity of the device owner and the telephone number of the device owner. See Hasebe at Col. 6, lines 49- 51." (Reply Br. 8.)

Such an admission shows no error in the Examiner's finding that Hasebe displays a message on a display of a processor-based device. Therefore, we affirm the rejection of claim 13.[1]

VI. ORDER

In summary, the rejection of claims 1-7 and 16-19 is reversed. The rejection of claims 9 and 11-15, however, is affirmed.

"Any arguments or authorities not included in the brief or a reply brief filed pursuant to [37 C.F.R.] § 41.41 will be refused consideration by the Board, unless good cause is shown." 37 C.F.R. § 41.37(c)(1)(vii). Accordingly, our affirmance is based only on the arguments made in the Briefs. Any arguments or authorities omitted therefrom are neither before us nor at issue but are considered waived. *Cf. In re Watts*, 354 F.3d 1362, 1367 (Fed. Cir. 2004) ("[I]t is important that the applicant challenging a decision not be permitted to raise arguments on appeal that were not presented to the Board.")

---

[1] Assuming *arguendo* that the prepositional phrase "to indicate that said processor-based device is not in possession of said rightful user" is entitled to patentable weight, we agree with the Examiner's finding that the reason Hasebe displays "data that identifies the information device owner" (col. 6, ll. 49-50) is to indicate the device is not in possession of its rightful owner, i.e., that it has been "lost or stolen . . . ." (Abs. ll. 24-26.)

No time for taking any action connected with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED-IN-PART

pgc

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins CO 80527-2400